Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

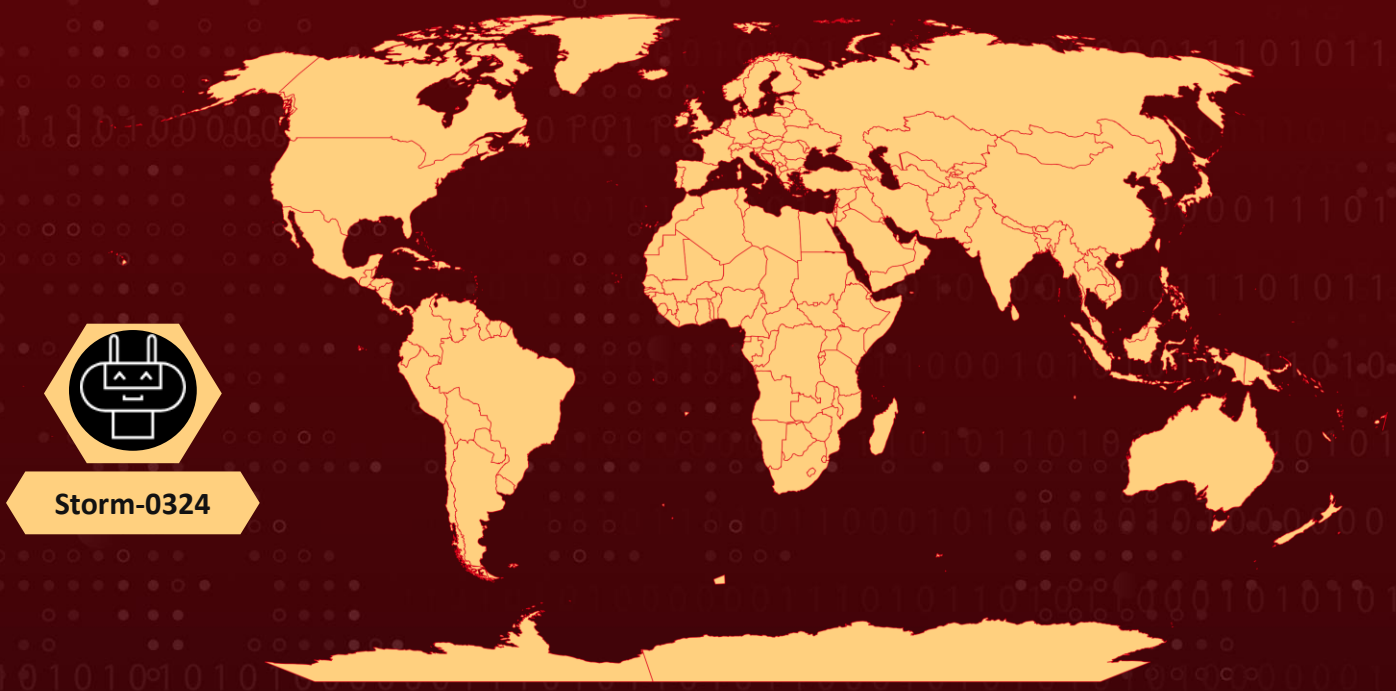
Storm-0324 Exploits Microsoft Teams Chats Deploying JSSLoader

Date of Publication	Admiralty code	TA Number
September 15, 2023	A1	TA2023373

Summary

Attack Began: July 2023
Actor Name: Storm-0324 (aka DEV-0324)
Target Industries: IT, Technology, High-Tech
Target Region: Worldwide
Malware: JSSLoader

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-21715	Microsoft Office Publisher Security Feature Bypass Vulnerability	Microsoft Teams	✓	✓	✓

Actor Details

#1 Storm-0324 (aka DEV-0324) is a financially motivated threat actor with a history of operating since 2016. This actor specializes in enabling ransomware deployments and granting access to compromised networks and devices to other threat actors. Notably, in 2019, Storm-0324 delivered its first payload to FIN7 (also known as Sangria Tempest), marking the beginning of their collaboration. Storm-0324 shares similarities with threat groups like TA543 and Sagrid.

#2 Starting from July 2023, Storm-0324 has shifted its focus to exploiting MS Teams chats through the use of an open-source tool. This tool is employed to distribute malicious payloads and send phishing lures, primarily in support of the activities of a specific cybercrime group called Sangria Tempest.

#3 Storm-0324's attack typically starts with phishing emails referencing payments or invoices. They utilize TeamsPhisher, an open-source Python tool for sending files to external tenants, as part of their tactics. These emails include a link to a SharePoint site hosting a ZIP archive containing a JavaScript file. Storm-0324 uses different file formats like WSF and Ekipa publisher files to host this code, relying heavily on the zero-day vulnerability CVE-2023-21715, a local security feature bypass vulnerability, in their attack strategy.

#4 Upon the execution of JavaScript, it triggers the deployment of a JSSLoader variant DLL. This JSSLoader malware is employed to facilitate initial access which is later handed-over to other sophisticated actor groups like FIN7. These sophisticated actors leverage initial access to establish C2, deploy ransomwares, and possess a formidable arsenal capable of wreaking havoc on systems.

#5 Microsoft has responded to this cyber threat by suspending all accounts and tenants that have been identified as linked to or exploited in this fraudulent behavior.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGETED INDUSTRIES
Storm-0324	Unknown **MOTIVE** Financial Gain	Worldwide	IT, Technology, High-Tech

Recommendations

Apply Patch: Install the security patch provided by Microsoft to address the CVE-2023-21715 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

Enhanced Email Security: Implement advanced spam filters, anti-phishing solutions, and email authentication protocols. Educate employees about identifying and reporting suspicious emails to prevent successful phishing attempts.

Least Privilege Access: Enforce the principle of least privilege (PoLP) to restrict user and application access rights to only what is necessary for their roles. This limits the potential damage if a system is compromised.

Cybersecurity awareness: Conduct regular cybersecurity awareness training sessions to educate employees about the risks associated with spear-phishing and social engineering tactics. Emphasize the importance of carefully scrutinizing email attachments, especially those received from unfamiliar or suspicious sources.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	T1566 Phishing	T1566.002 Spearphishing Link
T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1204 User Execution	T1204.001 Malicious Link
T1203 Exploitation for Client Execution			

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	67a1328242c89b2f54018d31eca071ab7edef6df30fea2633ad1a013aa5feb8a, 2373a6a7223154a2e4e3e84e4bdda0d5a9bc22580caf4f418dae5637efec65e5, 1f2ab2226f13be64feeece1884eaa46e46c097bb79b703f7d622d8ff1a91b938, 33b3a1da684efc2891668eecf883ba7b9768a117956786e4356a27d1dffe0560, c1e7d6ec47169ffb1118c4be5ecb492cd1ea34f3f3dd124500d337af3e980436, 15f15b643eafcc50777bed33eda25158c7f58f4dbaaaa511072ef913a302a8da, daba93cf353585a67ed893625755077a2d351ba46ec5ea86b5bd0b45b84bc7c5, 967882624ba26c4fcd6806791aa4994b5bf64ca4b1e66dd8d24f1fa54b3a43f0, 16f9674ea7c40a0e474966f59c413518509e295608c7ecc37c6096b034b88918, 2e3bc3b059733b4db846d3227abbfa6a7914b551f0175d6f77e22d08b57d49e3, a0c5b1fdcb95037e57dd502d848aa3137882d7af6fbf301262e8cd35db7f58b7, 2df508247a4e739b086c9de47d91a26ea7aee4d5cf9bc5cc70b5ad2dc7f102c6, d2b080b9af5d39d72af149afb065e769b1da8005edfe84237942a1b99f4fa36c, 793aa21ed7432ef2b0eda8d80036361878f728dbc4081d72f80fa3694702a4d8, 35f5c781d61d398ce47a8881228346a81afb4915bf083518bf2b4cc8d6a2685b, db1d98e9cca11beea4cfd1bfbe097dffd9fc4cc8b1b02e781863658d8c6f16c7, 410cd107dfd37752936bd20d022ea614cd373aa9d37db255f65dc434e653236a, 3b6d61add64402dc74d237e69d701ad2b0bea9a525798a376cd13f2090bb39ee, 969cfeddc1c90d36478f636ee31326e8f381518e725f88662cc28da439038001, ee8f394d9e192c453d47a0c57261a03921dcbb97248a67427cb6fc6d8833c8a0, 5450eca67cb31e326801df019d9a030d3bef8b04af6c91dadf760d62e2ca3ab1,

TYPE	VALUE
SHA256	10ce615d545a98a663de6419e11703fca20c150c8f1f6f0f90d5b0a04b49dfe9, 148d74e453e49bc21169b7cca683e5764d0f02941b705aaa147977ffd1501376, a062a71a6268af048e474c80133f84494d06a34573c491725599fe62b25be044, e0e8a8b3a807bad531cf98fa7ceaa57e43780cd67c3be1518de6d40023e22554, dd86898c784342fc11c42bea4c815cb536455ee709e7522fb64622d9171c465d, 7a17ef218eebfdd4d3e70add616adcd5b78105becd6616c88b79b261d1a78fdf, 98fe1d06e4c67a5a5666dd01d11e7342afc6f1c7b007c2ddbfc13779bcc51317, bf1371e2d79115fc7cfc89266cd7a59c02b04a74e1246435392eb5e20c661d8f, b08e713196b712c42da2df9da7836d270306065fbf6d4720f25d80e4104daf38, cc2171d14d0d3c4d117155185f7c911f781aac15b57adef6c32eb0149d5da3ba, bf1371e2d79115fc7cfc89266cd7a59c02b04a74e1246435392eb5e20c661d8f, dd86898c784342fc11c42bea4c815cb536455ee709e7522fb64622d9171c465d, b7beb0c0d33aaccd8b764082fde64676ead6c827e67a34fe0e6cf5fe28503cf6, daba93cf353585a67ed893625755077a2d351ba46ec5ea86b5bd0b45b84bc7c5, a0c5b1fdcb95037e57dd502d848aa3137882d7af6fbf301262e8cd35db7f58b7, 33b3a1da684efc2891668eecf883ba7b9768a117956786e4356a27d1dffe0560, 969cfeddc1c90d36478f636ee31326e8f381518e725f88662cc28da439038001, ee8f394d9e192c453d47a0c57261a03921dcbb97248a67427cb6fc6d8833c8a0, 5450eca67cb31e326801df019d9a030d3bef8b04af6c91dadf760d62e2ca3ab1, 5450eca67cb31e326801df019d9a030d3bef8b04af6c91dadf760d62e2ca3ab1, 10ce615d545a98a663de6419e11703fca20c150c8f1f6f0f90d5b0a04b49dfe9, 148d74e453e49bc21169b7cca683e5764d0f02941b705aaa147977ffd1501376, a062a71a6268af048e474c80133f84494d06a34573c491725599fe62b25be044,

TYPE	VALUE
SHA256	e0e8a8b3a807bad531cf98fa7ceaa57e43780cd67c3be1518de6d40023e22554, dd86898c784342fc11c42bea4c815cb536455ee709e7522fb64622d9171c465d, 7a17ef218eebfdd4d3e70add616adcd5b78105becd6616c88b79b261d1a78fdf, 98fe1d06e4c67a5a5666dd01d11e7342afc6f1c7b007c2ddbfc13779bcc51317, bf1371e2d79115fc7cfc89266cd7a59c02b04a74e1246435392eb5e20c661d8f, b08e713196b712c42da2df9da7836d270306065fbf6d4720f25d80e4104daf38, cc2171d14d0d3c4d117155185f7c911f781aac15b57adef6c32eb0149d5da3ba, bf1371e2d79115fc7cfc89266cd7a59c02b04a74e1246435392eb5e20c661d8f, dd86898c784342fc11c42bea4c815cb536455ee709e7522fb64622d9171c465d, b7beb0c0d33aaccd8b764082fde64676ead6c827e67a34fe0e6cf5fe28503cf6, daba93cf353585a67ed893625755077a2d351ba46ec5ea86b5bd0b45b84bc7c5, a0c5b1fdcb95037e57dd502d848aa3137882d7af6fbf301262e8cd35db7f58b7, 33b3a1da684efc2891668eecf883ba7b9768a117956786e4356a27d1dffe0560, 969cfeddc1c90d36478f636ee31326e8f381518e725f88662cc28da439038001, a062a71a6268af048e474c80133f84494d06a34573c491725599fe62b25be044, 1f2ab2226f13be64feeece1884eaa46e46c097bb79b703f7d622d8ff1a91b938, 15f15b643eafcc50777bed33eda25158c7f58f4dbaaaa511072ef913a302a8da, 793aa21ed7432ef2b0eda8d80036361878f728dbc4081d72f80fa3694702a4d8, 2df508247a4e739b086c9de47d91a26ea7aee4d5cf9bc5cc70b5ad2dc7f102c6, db1d98e9cca11beea4cfd1bfbe097dffd9fc4cc8b1b02e781863658d8c6f16c7, 61e84cf50024581d259c0c27dc4996f3777270259c29563755cf435f71467288, 98fe1d06e4c67a5a5666dd01d11e7342afc6f1c7b007c2ddbfc13779bcc51317, 148d74e453e49bc21169b7cca683e5764d0f02941b705aaa147977ffd1501376,

TYPE	VALUE
SHA256	c1e7d6ec47169ffb1118c4be5ecb492cd1ea34f3f3dd124500d337af3e980436, 16f9674ea7c40a0e474966f59c413518509e295608c7ecc37c6096b034b88918, 967882624ba26c4fcd6806791aa4994b5bf64ca4b1e66dd8d24f1fa54b3a43f0, 2373a6a7223154a2e4e3e84e4bdda0d5a9bc22580caf4f418dae5637efec65e5, d2b080b9af5d39d72af149afb065e769b1da8005edfe84237942a1b99f4fa36c, 2e3bc3b059733b4db846d3227abbfa6a7914b551f0175d6f77e22d08b57d49e3, 7a17ef218eebfdd4d3e70add616adcd5b78105becd6616c88b79b261d1a78fdf, 2cabfffda2b1f1202d551d16d7edbdb77c37363f08136e8962fa9f4d224e4027, 16f9674ea7c40a0e474966f59c413518509e295608c7ecc37c6096b034b88918, 148d74e453e49bc21169b7cca683e5764d0f02941b705aaa147977ffd1501376, 2df508247a4e739b086c9de47d91a26ea7aee4d5cf9bc5cc70b5ad2dc7f102c6, d2b080b9af5d39d72af149afb065e769b1da8005edfe84237942a1b99f4fa36c, 6f9a4e87db50896fb4f54ea3e85f015bac383faf0e3db0f5b20c462f322e946a, 3d7199f569a31d3826afd04a2f7d4dd2f692c9731fdf8cdfc8c7e03626bffdaf, c1e7d6ec47169ffb1118c4be5ecb492cd1ea34f3f3dd124500d337af3e980436, c2e6f2496ab549c258a1d004fb0c5548413c81f5a556611c369d93a75e3835be, 15f15b643eafcc50777bed33eda25158c7f58f4dbaaaa511072ef913a302a8da, 98fe1d06e4c67a5a5666dd01d11e7342afc6f1c7b007c2ddbfc13779bcc51317, 55e29ad1d04af6fd59592825681438f2ba262751de14d64d9cf41c89d8ad6294, 1f2ab2226f13be64feeece1884eaa46e46c097bb79b703f7d622d8ff1a91b938, 2180d0f46ec6f843fa8b1984acfd251371be7d4228d208eb22bc4a87e9b7c59f, 6a75254b45320109090fd775dcb78ec4e3dbcf325c3916253b5d6e105b92be66, e6d239a37a39b8051e40949fa4647efa6dd990a3afe27e381f1e1eea17d6b17b,

TYPE	VALUE
SHA256	a0c5b1fdcb95037e57dd502d848aa3137882d7af6fbf301262e8cd35db7f58b7, 33b3a1da684efc2891668eecf883ba7b9768a117956786e4356a27d1dffe0560, 263b665a2cf660dc6b9f641e0ed5bf28023b81b6d1b48fc849aae57b025288e7e, daba93cf353585a67ed893625755077a2d351ba46ec5ea86b5bd0b45b84bc7c5, 49895428f1a30131308022dd3aa56eab6a1aa49b08a978ebc1520e289d3d6744, db1d98e9cca11beea4cfd1bfbe097dffd9fc4cc8b1b02e781863658d8c6f16c7, 2373a6a7223154a2e4e3e84e4bdda0d5a9bc22580caf4f418dae5637efec65e5, 2e3bc3b059733b4db846d3227abbfa6a7914b551f0175d6f77e22d08b57d49e3, 793aa21ed7432ef2b0eda8d80036361878f728dbc4081d72f80fa3694702a4d8, 969cfeddc1c90d36478f636ee31326e8f381518e725f88662cc28da439038001, a062a71a6268af048e474c80133f84494d06a34573c491725599fe62b25be044, c328f48c5f4a2c2441bcd0b0c0551547ca254f7ebbb46d30d357e962d8330063, 8279ce0eb52a9f5b5ab02322d1bb7cc9cb5b242b7359c3d4d754687069fcb7b8, 967882624ba26c4fcd6806791aa4994b5bf64ca4b1e66dd8d24f1fa54b3a43f0

Patch Link

https://msrc.microsoft.com/update-guide/en-us/advisory/CVE-2023-21715

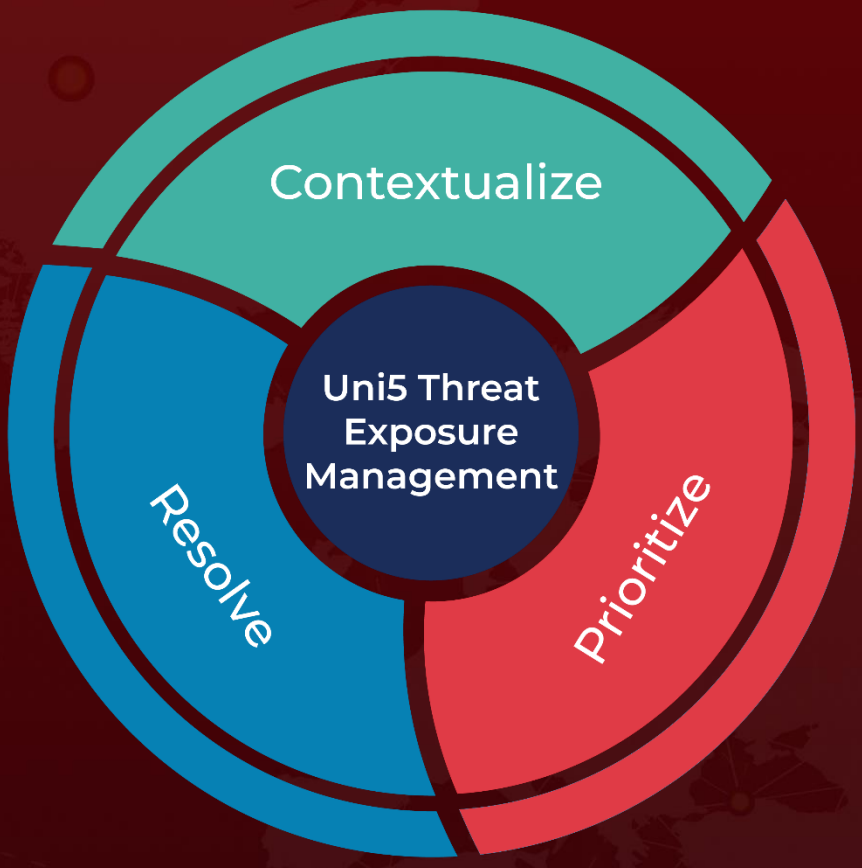
References

https://www.microsoft.com/en-us/security/blog/2023/09/12/malware-distributor-storm-0324-facilitates-ransomware-access/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 15, 2023 . 7:10 AM

More at www.hivepro.com